



(19) RU (11) 2097931 (13) C1

(51) 6 H 04 L 9/00

Комитет Российской Федерации
по патентам и товарным знакам

ВСЕРОССИЙСКАЯ
ПАТЕНТНО-ТЕХНИЧЕСКАЯ
БИБЛИОТЕКА

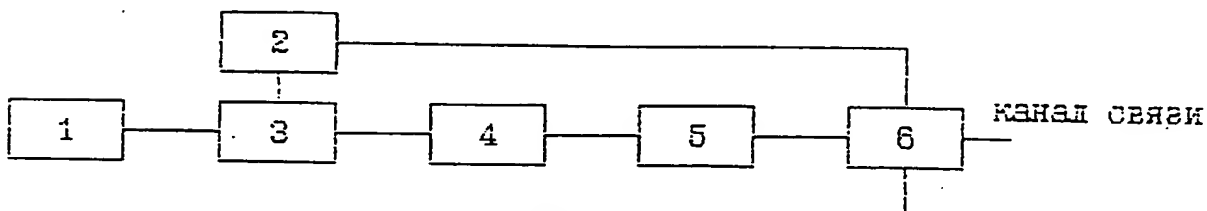
(12) **ОПИСАНИЕ ИЗОБРЕТЕНИЯ**
к патенту Российской Федерации

1

(21) 95100567/09 (22) 12.01.95
(46) 27.11.97 Бюл. № 33
(76) Березин Борис Владимирович, Волков
Сергей Сергеевич, Рощин Борис Васильевич,
Сердюков Петр Николаевич
(56) 1. Сяо Д., Керр Д., Мэдник С. Защита
ЭВМ. - М.: Мир, 1982, с.137 - 162.
(54) СПОСОБ ШИФРОВАНИЯ ДВОИЧ-
НОЙ ИНФОРМАЦИИ И УСТРОЙСТВО
ДЛЯ ЕГО ОСУЩЕСТВЛЕНИЯ
(57) Изобретение относится к криптографи-
ческим преобразованиям и может быть
использовано в связных, вычислительных и
информационных системах для криптографи-
ческого закрытия двоичной информации.

2

Технический результат - обеспечение побит-
ного шифрования информации с использо-
ванием ключа необходимого пользователю
размера. Сущность изобретения заключается
в многократном прибавлении ключа к
преобразуемой информации с последующим
применением подстановочных и перестано-
вочных преобразований. Устройство содержит
на передаче и приеме p -разрядный ключевой
регистр 1, p -разрядный регистр сдвига 2,
 p -разрядный сумматор 3, блок 4 разрядного
функционального преобразования f , мажори-
тарный элемент 5, однородный сумматор. 2
с. и 2 з.п. ф-лы, 2 ил.



Фиг. 1.

RU

2097931

C1

RU

2097931

C1

Изобретение относится к криптографическим преобразованиям и может быть использовано в связных, вычислительных и информационных системах для криптографического закрытия двоичной информации.

Известен способ шифрования, предназначенный для криптографической защиты информации в системах связи и вычислительных системах и заключающийся в многократном прибавлении ключа к преобразуемой информации с последующим применением подстановочных и перестановочных преобразований. С использованием этого способа построена система Lucifer фирмы IBM и стандарт шифрования данных Национального бюро стандартов США.

В известном стандарте шифрования данных к содержимому двух 32-разрядных ячеек 64-разрядного информационного регистра 16 раз прибавляют по модулю 2 содержимое 64-разрядного ключевого регистра с последующим воздействием на 32-разрядную сумму 32-разрядным функциональным преобразованием f .

Известный стандарт шифрования данных шифрует информацию блоками по 64 бита, а это при зашифровании требует предварительного накапливания 64 бит информации, а при расшифровании требует дополнительной синхронизации для выделения начала очередного блока зашифрованной информации. Кроме того, процесс зашифрования очередного блока состоит из 16-и циклов, что вносит определенную задержку при зашифровании очередных блоков информации. Перечисленные особенности известного стандарта шифрования данных делают его неудобным при использовании в системах радиосвязи.

Целью настоящего изобретения является обеспечение побитного шифрования информации с использованием ключа необходимого пользователю размера.

Поставленная цель достигается тем, что в способе шифрования двоичной информации, заключающемся в зависящем от 64-разрядного ключа преобразовании 64-разрядного блока шифруемой информации путем 16-кратного выполнения набора операций, включающего сложение 32-разрядных чисел из информационного и ключевого регистра и функциональное преобразование полученной 32-разрядной суммы, на передаче p -разрядные содержимые p -разрядного ключевого регистра и p -разрядного регистра сдвига складывают (например по модулю 2 либо 2^n), сумму преобразуют блоком p -раз-

рядного функционального преобразования f , в полученном p -разрядном результате преобразования мажоритарным элементом определяют преобладание нулей или единиц и в зависимости от результата прибавляют по модулю 2 к двоичному знаку шифруемой информации соответственно 0 или 1, полученный в результате зашифрованный двоичный знак направляют в канал связи и на вход p -разрядного регистра сдвига, а на приеме выполняют те же действия, что и на передаче, за исключением того, что на вход p -разрядного регистра сдвига направляют пришедший из канала связи зашифрованный двоичный знак, к которому одновременно прибавляют по модулю 2 выработанный мажоритарным элементом двоичный знак и получают знак открытой информации. Чтобы мажоритарный элемент однозначно реагировал на поступающее на его вход число, разрядность числа p выбирается нечетной.

На фиг. 1 и 2 представлены соответственно блок-схемы устройств зашифрования и расшифрования для осуществления способа шифрования двоичной информации.

Устройства зашифрования и расшифрования содержат p -разрядный ключевой регистр 1, p -разрядный регистр сдвига 2, p -разрядный сумматор 3, блок p -разрядного функционального преобразования 4, мажоритарный элемент 5 и одноразрядный сумматор 6.

Процесс зашифрования бита открытой информации осуществляют следующим образом.

p -Разрядные содержимые p -разрядного ключевого регистра 1 и p -разрядного регистра сдвига 2 складывают (например по модулю 2 либо 2^n) в p -разрядном сумматоре 3, полученную сумму преобразуют блоком 4 p -разрядного функционального преобразования f , мажоритарным элементом 5 определяют количество единиц в p -разрядном результате преобразования. Если единиц больше, чем нулей, то в одноразрядном сумматоре 6 к двоичному знаку открытой информации прибавляют 1, в противном случае - 0. Полученный в результате суммирования двоичный знак зашифрованной информации направляют в канал связи и на вход p -разрядного регистра сдвига 2, содержимое которого предварительно сдвигают на один разряд в сторону младших разрядов с потерей выдвинутого самого младшего разряда.

Процесс расшифрования бита зашифрованной информации осуществляют следующим образом.

n -Разрядные содержимые n -разрядного ключевого регистра 1 и n -разрядного регистра сдвига 2 складывают в n -разрядном сумматоре 3, полученную сумму преобразуют блоком 4 n -разрядного функционального преобразования f , мажоритарным элементом 5 определяют количество единиц в n -разрядном результате преобразования. Если единиц больше, чем нулей, то в одноразрядном сумматоре 6 к пришедшему из канала связи знаку зашифрованной информации прибавляют 1, в противном случае - 0. В результате суммирования получают двоичный знак открытой информации. Пришедший из канала связи знак зашифрованной информации одновременно направляют на вход n -разрядного регистра сдвига 2, содержимое которого предварительно сдвигают на один разряд в сторону младших разрядов с потерей выдвинутого самого младшего разряда.

Если в i -й момент n -разрядный ключевой регистр 1 содержит n -разрядное число $k(i) = (k_1(i), \dots, k_n(i))$, $k_j(i) = 0, 1$, $1 \leq j \leq n$, $i \geq 1$, то в i -й момент мажоритарный элемент вырабатывает двоичный знак $\gamma(i) = M(f(a(i) + k(i)))$, где $M(a) = \{0, \text{если } |a| < n/2; 1, \text{если } |a| > n/2\}$, $|a|$ - количество единиц в n -разрядном двоичном числе a .

Если $o(i) = i$ -й двоичный знак открытой информации, $\pi(i)$ - i -й двоичный знак

зашифрованной информации, то $\pi(i) = o(i) \oplus \gamma(i)$ на передаче и $o(i) = \pi(i) \oplus \gamma(i)$ на приеме.

Содержимое n -разрядного регистра сдвига 2 в $(i+1)$ -й момент станет $c(i+1) = (c_1(i+1), \dots, c_n(i+1)) = \pi(i)$.

Содержимое n -разрядного ключевого регистра 1 от такта к такту можно обновлять, например, при помощи регистра сдвига с линейной функцией в обратной связи. Если характеристический многочлен регистра име-

ет вид $1 \otimes x^{1-1} \otimes \dots \otimes x^{1-1n} \otimes x$, то в $(i+1)$ -й момент содержимое n -разрядного ключевого регистра 1 станет $k(i+1) = (k_1(i+1), \dots, k_n(i+1)) = (k_n(i), k_1(i+1) = k_1(i) \otimes k_1(i) \otimes \dots \otimes k_1(i))$.

В качестве n -разрядного функционального преобразования f можно выбрать, например, прибавление по модулю 2^n к преобразуемому n -разрядному числу $x = (x_1, \dots, x_n)$ n -разрядной константы a или n -разрядной константы b в зависимости от четности количества единиц в преобразуемом n -разрядном числе. Тогда $f(x) = x + x' \cdot a + (x' \otimes 1) \cdot b$,

где $x' = \bigoplus_{j=1}^n x_j$, $a = 2^{n-2} + 2^{n-4} + \dots + 2^2 + 2^0$, $b = 2^{n-2} + 2^{n-4} + \dots + 2^2 + 2^0 + 1$.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ шифрования двоичной информации, заключающийся в зависящем от 64-разрядного ключа преобразования на передаче и приеме 64-разрядного блока шифруемой информации путем 16-кратного выполнения набора операций, включающего сложение 32-разрядных чисел из информационного и ключевого регистров и функциональное преобразование полученной 32-разрядной суммы, отличающийся тем, что на передаче n -разрядные содержимые n -разрядного ключевого регистра и n -разрядного регистра сдвига суммируют, полученную сумму преобразуют блоком n -разрядного функционального преобразования f , в полученном n -разрядном результате преобразования мажоритарным элементом определяют преобладание нулей и единиц и в зависимости от результата прибавляют по модулю 2 к двоичному знаку шифруемой информации соответственно 0 или 1, полученный в результате зашифрованный двоичный знак направляют в канал связи и на вход n -разрядного регистра сдвига, а на приеме n -разрядные содержимые n -разрядного клю-

чевого регистра и n -разрядного регистра сдвига складывают, полученную сумму преобразуют блоком n -разрядного функционально преобразования f , в полученном n -разрядном результате преобразования мажоритарным элементом определяют преобладание нулей и единиц и в зависимости от результата прибавляют по модулю 2 соответственно 0 или 1 к пришедшему из канала связи зашифрованному двоичному знаку, который одновременно направляют на вход n -разрядного регистра сдвига.

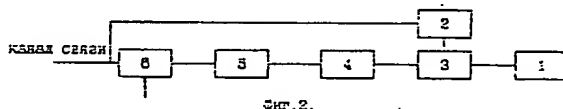
2. Способ по п.1, отличающийся тем, что блок функционального преобразования f в зависимости от четности количества нулевых разрядов в n -разрядном преобразуемом числе прибавляют по модулю 2^n к преобразуемому числу n -разрядную константу a или n -разрядную константу b .

3. Устройство шифрования двоичной информации, содержащее на приеме и передаче 8 n -разрядный ключевой регистр, 8-разрядный блок функционального преобразования f и два 8-разрядных сумматора, отличающееся тем, что на приеме и

передаче введены p -разрядный регистр сдвига и мажоритарный элемент, вырабатывающий знак 0 при передаче на его вход p -разрядного числа с преобладанием нулевых разрядов и знак 1 при подаче на вход мажоритарного элемента p -разрядного числа с преобладанием единичных разрядов, при этом ключевой регистр выполнен в виде p -разрядного ($p = 1, 3, 5 \dots$) ключевого регистра, блок функционального преобразования выполнен в виде блока p -разрядного функционального преобразования f , первый сумматор выполнен в виде p -разрядного сумматора, а второй сумматор - в виде одноразрядного сумматора, причем на передаче выход p -разрядного ключевого регистра подключен к первому входу p -разрядного сумматора, второй вход которого подключен к выходу p -разрядного регистра сдвига, вход которого подключен к выходу одноразрядного сумматора, вход которого подключен к выходу мажоритарного

элемента, вход которого подключен к выходу блока p -разрядного функционального преобразования f , вход которого подключен к выходу p -разрядного сумматора, а на приеме выход p -разрядного ключевого регистра подключен к первому входу p -разрядного сумматора, второй вход которого подключен к выходу p -разрядного регистра сдвига, а выход p -разрядного сумматора подключен к входу блока p -разрядного функционального преобразования f , выход которого подключен к входу мажоритарного элемента, выход которого подключен к входу одноразрядного сумматора.

4. Устройство по п.3, отличающееся тем, что p -разрядный ключевой регистр выполнен в виде p -разрядного регистра сдвига с обратной связью с линейной функцией в обратной связи.



Best Available Copy

Заказ 374 Подписное
ВНИИПИ, Рег. ЛР № 040720
113834, ГСП, Москва, Раушская наб., 4/5

121873, Москва, Бережковская наб., 24 стр. 2.
Производственное предприятие «Патент»